EXHIBIT 58

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION,
PLAINTIFF,
vs.
SOLARWINDS CORP. AND TIMOTHY G. BROWN,
DEFENDANTS.

Case No. 23-cv-9518-PAE

VIDEOTAPED DEPOSITION OF
BRENT THILL
Wednesday, August 28, 2024
San Francisco, California

Reported By:
KATHLEEN A. MALTBIE, STENOGRAPHIC REPORTER
California CSR 10068, Nevada CCR 995, Texas CSR 12212, RPR-RMR-CRR-CCRR-CLR-CRC-RDR
JOB No. 240828KWI

VIDEOTAPED DEPOSITION OF BRENT THILL
BE IT REMEMBERED that on Wednesday, August 28, 2024, commencing at the hour of 9:06 a.m. thereof, before me, Kathleen A. Maltbie, RPR-RMR-CRR-CCRR-CLR-CRC-RDR, a Certified Stenographic Shorthand Reporter, in and for the State of California, Nevada and Texas, personally appeared BRENT THILL, a witness in the above-entitled court and cause, who, being by me first duly sworn, was thereupon examined as a witness in said action.

APPEARANCES OF COUNSEL

FOR THE PLAINTIFF:
SECURITIES AND EXCHANGE COMMISSION
100 F Street, N.E.
Washington, D.C. 20549
BY: CHRISTOPHER BRUCKMANN, ESQ.
BENJAMIN BRUTLAG, ESQ.
Telephone: (202) 256-7941
Email: BruckmannC@sec.gov
brutlagb@sec.gov

FOR THE DEFENDANTS:

LATHAM & WATKINS, LLP
1271 Avenue of the Americas
New York, New York 10020
BY: SERRIN TURNER, ESQ.
JOSH KATZ, ESQ.
Telephone: (212) 906-1330
Email: Serrin.turner@lw.com
Josh.Katz@lw.com
LATHAM & WATKINS, LLP
330 North Wabash Avenue, Suite 2800
Chicago, Illinois 60611
BY: KIRSTEN C. LEE, ESQ. (Zoom)
Telephone: (312) 777-7281
Email: Kirsten.lee@lw.com

FOR JEFFERIES AND THE WITNESS:

WILMERHALE
1 Front Street, Suite 3500
San Francisco, California 94111
BY: MICHAEL MUGMOM, ESQ.
Telephone: (628) 235-1006
Email: Michael.mugmon@wilmerhale.com
WILMERHALE
60 State Street
Boston, Massachusetts 02109
BY: JESSICA NOTEBAERT, ESQ.
Telephone: (617) 526-6721
Email: Jessica.notebaert@wilmerhale.com

APPEARANCES (Continued)

ALSO PRESENT:

Frank Quirarte, Videographer
Greg Rose, Jefferies (Zoom)

MR. BRUCKMANN: Yes. For the record, I have no more questions for Mr. Thill, so I'm passing the witness to Mr. Turner.
MR. TURNER: Thanks.
EXAMINATION BY MR. TURNER
BY MR. TURNER:
Q. Good afternoon, Mr. Thill.
A. Good afternoon.
Q. I'll try to be efficient in my questions. I know you're busy.
Let me start by asking you, as an analyst, you research issues that you -- you think will be important to your investor clients, right?
A. Right.
Q. And -- and I think you testified you can do that lots of different ways.
You talk to customers; yes?
A. Yes.
Q. And experts?
A. Yes.
Q. You read the company's SEC filings?
A. (Nods head.)
Q. "Yes"?
A. Yes.
Q. You have to answer yes or no.

A. Yes.
Q. You read relevant material in the company's website?
A. Yes.
Q. Talk -- you can talk to the management team?
A. Yes.
Q. I think you've said you also sometimes talk to product managers?
A. Yes.
Q. Which are below the management team, right?
A. Yes.
Q. You can ask questions on earnings calls?
A. Yes.
Q. And I think you said you research everything that would go into an investor's decision to buy stock or not?
A. Yes.
Q. You don't assume the company is going to turn a profit?
One of the things you would research?
A. Yes.
Q. You don't assume companies' products are as good as the companies say they are?

A. Yes.
Q. You don't assume the competition is as weak as the company may think it is?
A. Yes.
Q. You try to research all those issues the best you can so you can draw your own conclusions?
A. Correct.
Q. Now, you testified that cyber security is incredibly important, you said several times. And I just want to zero in on what you mean by that.
I gather what you mean is that cyber incidents can have a damaging effect on a company's business?
A. Correct.
Q. You mentioned the delta incident, for example?
A. Correct.
Q. But you don't mean, do you, that a company's internal cyber security practices are an incredibly important factor that you yourself research when you analyze a company?
MR. BRUCKMANN: Objection.
THE WITNESS: We don't research it because we assume that companies are following a process and procedure. So we don't spend a lot of time on that

topic because it's not -- it's important to our clients because there are other factors that are more important that are -- that are on the top of their radar.
BY MR. TURNER:
Q. I'll come back to the assumption in a minute, but I just want to confirm, this is not an incredibly important issue that you research as part of your work as an analyst?
A. We don't research it specifically in depth because we don't -- we don't do that because we are assuming that companies are -- are handling it in the best way that they can.
Q. I get the assumption.
A. Yes.
Q. I'd just like an answer to my question, which is, it's not an incredibly important research topic that you yourself research or your team?
A. We do not research it, but it is important.
Q. It's important in the sense that cyber security, if you have a cyber security failure --
A. Right.
Q. -- can damage a business?
A. If we want --

Q. Let me finish.
But it's not something that when you're doing your research, it's incredibly important for you to research yourself?
A. It's not part of our research process where we go in with a microscope on cyber security in any report we've ever published.
Q. It's not just going in with a microscope, Mr. Thill. You didn't even look at the security statement that just posted publicly on the company's website, right?
I mean, you don't even do that level of research?
A. We have seen the statement, but it's a generic statement. It's a statement that's on virtually every company's website.
Q. Just to be clear, you -- you did not even see this statement at the time that you were looking into SolarWinds?
A. Not that I recall.
Q. You haven't seen the security statement before this litigation?
A. Not that I recall.
Q. So, again, even that surface-level information is not information that you or your team

seek out when you're doing research on a company?
A. No. Because it's a given that we believe that these processes and procedures are in place.
Q. Right.
And I promise I'm going to get to the assumption later on, but I just want a clear answer to my question.
A. No.
Q. Thank you.
And just to be clear, it was material that you could have looked up at the time, but did not?
A. I don't -- I don't think there's anything material about -- about it. In -- in most situations, what happens is, when we sit down with the team, a management team, we have an understanding who they are. We'll ask them, hey, is there -- are there any big issues, any big concerns. And given that I knew your CEO from his red hat days, I viewed him as credible and a thoughtful individual that did the right thing for his -- his customers and shareholders. So it never really came up in the questioning.
Q. Just to be clear, I'm not suggesting there was anything wrong with you not looking into this. I just want to get the facts.

So you said, I think earlier, that --
A. It's --
Q. Let me just finish my question. Sorry.
When you're looking at a company, often you look at the website for information about products, for information about events, all sorts of information. But you never sought out SolarWinds' security statement from its website when you were doing research on the company; is that correct?
A. At the time, correct. Going forward, it's become more part of the checklist because of the magnitude of some of these breaches that we've been seeing, so --
Q. Just to be clear, I'm talking about the time frame --
A. Was not --
Q. -- 2018 to --
A. It was not.
Q. You wouldn't --
A. It was not -- it was not part of the process. Right or wrong, it was not part of the process.
Q. Sure.
And you mentioned you could talk to Kevin Thompson or members of the management team.

You never asked them to supply information about the company's internal cyber security procedures?
A. No.
Q. And you mentioned product managers.
You never asked to speak with product managers about their view of the company's security practices?
A. No.
Q. And just to be clear, you -- you spoke with the CEO, and I think you said the CFO?
A. CEO, CFO, investor relations are our primary contacts across the majority of our companies.
Q. Okay. And the company also has a chief technology officer and a chief information officer, but you never asked to speak to them, as far as you can recall?
A. Unclear. And I'm sure at analyst days or events, we -- we've had interaction, but we never sought out anyone to -- to cover those topics at that point.
Q. To "cover those topics," meaning the company's internal cyber security practices?
A. Correct.
Q. And I assume that's your general practice.

It's not just SolarWinds, in researching the companies you follow, you just don't study the internal cyber security practices of those companies?
A. No. And neither do our buy side clients. So I can say, after 25 years, I've never been asked by a buy sider, how would you grade their cyber hygiene. We've never -- we've never been asked that by our clients. Again, not -- not saying it's not something you should be -- but it's not -- not been at the top of their list.
Q. And I assume for the same reasons, in the reports that you issued about SolarWinds, you never mentioned anything about their internal cyber security controls?
A. No.
Q. And I -- I assume your general practice, can you recall any investor report you've put out that is focused on a company's internal cyber security controls?
A. No. Only if there was a material issue, we would comment about it if there was a -- a breach that was publicly made available by the company.
Q. Right.
And I think you said before, that's really

what you're concerned about. It's not so much whether every check box has been checked internally, but it's more about has a damaging breach occurred?
A. Correct.
Q. Now, you've repeatedly said that you assume that every company has good cyber security practices in place, and just like you assume the water you drink is safe.
Do you remembering that testimony?
A. Yes.
Q. I just want to push on that a little bit because, honestly, I'm not sure that's exactly what you mean.
You testified today that many companies, including tech companies, have suffered cyber security incidents?
A. Yes.
Q. You mentioned Adobe?
A. Yes.
Q. Microsoft?
A. Yes.
Q. These are major tech companies, right?
MR. MUGMON: And you can let him ask a question before you -- you answer. I'm not sure these were specific questions.

MR. TURNER: They were meant to be. That's fine. I'll let you know if you need to hold off.
THE WITNESS: He scolded me already.
BY MR. TURNER:
Q. These are major tech companies, right?
A. Yes.
Q. I think even CrowdStrike you mentioned, a cyber security company, recently they had a major cyber security incident?
A. Yes.
Q. I think you said specifically every major software company has been hacked; yes?
A. Yes.
Q. Everyone is going through this across the industry?
A. Correct.
Q. It's fair to say, right, this is not even limited to companies, but even the most sophisticated government agencies, like the NSA, have repeatedly been hacked?
A. Yes.
Q. And dare I say, even the SEC itself has been hacked on multiple occasions?
A. I'm unaware of that, but ...

Q. You haven't heard of their Edgar system being hacked?
A. I have not.
Q. You haven't heard of their Twitter account being hacked?
A. I have not.
Q. Check the -- the news when you have a minute.
But fair to say, you -- you don't really assume that every software company out there is safe.
The evidence is clear that they're not?
A. The bad guys are getting more sophisticated.
Q. And as a result, they're getting into companies?
A. Correct.
Q. So, again, you don't really assume that every company out there is safe?
A. We assume that they're doing the best that they can to protect themselves against threats. I'm not by default saying that they're all safe.
Q. I think, is it fair to say, what you mean is that you assume companies have reasonable cyber security practices in place because you don't have

the expertise to analyze that issue, so it's not an issue that you look at?
A. It's not -- it's -- I'm not a security expert.
Q. Yeah. So it's not something you look at?
A. I'm a financial analyst.
Q. Exactly.
So it's not something you look at specifically in your research, but you're not really assuming, oh, yeah, they're never going to be attacked?
A. We don't make -- no. We -- we -- we -- I think the assumption that, based on what we've seen, that everyone is going to have an incident. When the number one security company, CrowdStrike, brings down an entire airline, the only thing you can do is, by default, someone is going to get attacked, and -- and there's going to be -- there's going to be issues. It's a question of what do they do with the issue.
Q. Yeah.
A. How do you deal with the issue.
Q. Have you ever heard the -- the saying, with -- with relation to cyber security that it's not a question of if, but when?

A. Correct. Yes. We've --
Q. So it sounds like you really assume that companies are unsafe, but it's just not an issue that you have the ability to look into, so you just put it to the side when you're doing your research and don't look -- look into it yourself?
A. It's back burner, but we are aware of and want to understand -- we want to understand more about it, but it's not an area where, again, I've -- I've spent a lot of time going in to make the assessment to our clients.
Q. And I just want to focus, again, on the, you know, 2018 to '21 period.
During that period, you weren't asking for information about it?
A. No.
Q. All right.
A. We weren't being asked by our clients for it either.
Q. And you weren't assuming companies were safe back then, again, you were just assuming it was not an issue you could really look into yourself and, therefore, you were bracketing it in your analysis --
A. Yes.

Q. -- fair?
Now, the SEC showed you a series of internal SolarWinds documents, right?
A. Yes.
Q. These sort of documents are not the type of documents that you would generally analyze or be asked to analyze?
A. No.
Q. And before disclosing information to investors in SEC filings or earnings calls, like, companies usually have procedures to vet the information to make sure it's accurate, right?
A. Correct.
Q. Companies just don't, you know, dump a bunch of internal emails or -- or PowerPoint decks or spreadsheets on investors and -- and ask them to figure out the facts themselves?
A. No, they don't.
Q. That would be confusing, wouldn't it?
A. It's -- yeah. It's confusing, just takes time to process and you have to build context behind it.
Q. Yeah.
Relying on documents like that would be risky if you don't have all the relevant context?

A. Correct.
Q. So if -- if one of the documents that you were shown here today somehow was magically dropped in your lap, you would want to make sure you had all the relevant context before you relied on it in advising your investors, right?
A. Yes.
Q. You need more context to understand what the purpose of the document was?
A. Yes.
Q. About the issue being discussed?
A. Yes.
Q. What was meant by certain remarks?
A. Yes.
Q. Whether the person who made the remark had all the relevant facts themselves?
A. Yes.
Q. And you don't know, do you, whether you have all the context that you need to accurately understand the internal documents that have been shown to you here today?
A. I don't.
Q. Let me show you one of the documents, Exhibit 7.
We'll turn back to the page Bates stamped

ending in -11.
And I believe you were pointed to a specific bullet point at the top, and then the number 1 in the chart below, right?
A. Yes.
Q. Again, if -- if this landed in your lap, you would not run out and tell investors to sell SolarWinds stock?
A. No. It doesn't have an impact on -- on my recommendation on -- on its own.
Q. Yeah, you would want to talk to the person who prepared the document, if you could, to find out what was meant by this?
A. Correct.
Q. I can represent to you that the company's CIO, chief information officer, Rani Johnson, testified in the case yesterday. Deposition Mr. Bruckmann was present at, and she testified that she participated in preparing this document.
I want to ask you, would it change your view of the significance of this statement -- let me put it differently.
Would you want to know that Ms. Johnson testified that this remark and this number were not about any lack of access controls, but instead were

about a really shorthand reference to an ongoing project to standardize how access was being managed at the company?
Would that be important to you --
MR. MUGMON: Objection. Calls for speculation.
BY MR. TURNER:
Q. -- to know?
A. We -- we'd want more -- we would want more details behind it and be helpful to hear both sides rather than just seeing the doc, hearing your perspective.
Q. Most importantly, the perspective of the person who actually wrote the words, right?
A. We'd like -- yeah. We'd like to hear from that person.
Q. Yeah. If that person testified that this was not about a lack of access controls, but instead about making the company's access management technology consistent across the company's business lines, that would be significant context you'd want to know?
MR. MUGMON: Objection. Calls for speculation.
THE WITNESS: It would be helpful, but I'd

want to hear more from her about it.
BY MR. TURNER:
Q. Sure.
And I'll show you Exhibit 10 here. Turning to page Bates stamped -1611.
MR. MUGMON: I'm sorry, which page was it?
MR. TURNER: -1611.
MR. MUGMON: Thank you.
BY MR. TURNER:
Q. You were pointed to this very short remark in here saying significant deficiencies in user access management.
Remember that?
A. Yes.
Q. Again, would it be helpful context for you to know that Miss Rani -- excuse me -- Ms. Johnson testified yesterday that, again, this statement had nothing to do with the quality of SolarWinds' access controls?
MR. BRUCKMANN: Objection.
BY MR. TURNER:
Q. Would that be significant context for you to know?
A. Yeah. It would be great to hear more about what's behind the slide.

Q. Would it be --
A. It's a statement on a slide, so we'd want to hear everyone's perspective on it.
Q. Would it be helpful to know that Ms. Johnson testified this statement was about deficiencies in the way that user access was audited for SOX purposes on a single occasion?
A. Yes. Love to hear that context.
Q. And the audit was re-done using the proper procedures after the issue was discovered.
Would that be helpful context to know?
A. Yes.
Q. I think you said in your testimony you saw a trend line in some of the documents you saw today?
A. Yes.
Q. And I gather what you meant, you saw the same numbers showing up in certain documents that the SEC put in front of you?
A. That, and then there's a trend line here. It seems like the overall category score is going higher, which is a good thing to see.
Q. Right.
You're -- you're pointing to the up --
A. Overall.
Q. -- in -1611.

But in terms of the -- the number 1s that you were pointed to on access controls or related to access controls, at least that's the way it was presented to you, you don't know if those notations referred to the same issue or not?
A. No idea.
Q. You don't know exactly what the issue was underlying any particular notation?
A. No.
Q. So you don't have any reliable basis to conclude that there was any specific trend at the company related to access controls?
A. No. Other than the word "access control" was used many places and the score was low.
Q. I want to go back to the security statement.
We don't need to look at it.
You stated that you would assume that SolarWinds had practices like these in place, right?
A. Every company has that in place, I would believe.
Q. Pretty basic policies?
A. Yeah.
Q. But I -- I also -- is it fair to say you would not assume that these policies were perfectly

implemented all the time?
A. I wouldn't expect them to be perfect.
Q. Yeah.
I think you even said that none of these companies are perfect?
A. Right.
Q. Meaning, none -- no company gets security right all the time?
A. Correct.
Q. What's most important is that a company had these policies generally in place, but was always looking for gaps and finding -- and fixing any that it found?
A. Yes.
Q. That's what a good cyber security program does?
A. Yes.
Q. And anyone who's knowledgeable about the industry would understand that when they read the security statement, right?
A. Yes. No one would score perfect across the whole board.
Q. Going back to the -- what we discussed earlier, that the biggest issue for you is not so much whether every check box is checked, but whether

a material breach has occurred at the company.
SolarWinds advised investors that it was at risk of a cyber security incident.
Are you -- are you aware of that?
A. No.
Q. You read SolarWinds' investor filings, though, right?
A. Yes.
Q. Including its risk disclosures?
A. I don't -- I don't read every risk disclosure perfectly, but I'll -- generally, it's part of -- part of every -- every one of your documents.
MR. TURNER: Let me mark this, I forget where we are in the chain.
THE REPORTER: 13.
MR. TURNER: Let me mark this as 13, please.
(Whereupon, Deposition Exhibit 13 was marked for identification.)
BY MR. TURNER:
Q. So do you recognize that this is an excerpt from the company's risk disclosures?
Is that what it appears to you?
A. Yes.

Q. This is from 2019.
So turning to the -- let's see here -- third page of the exhibit, do you see under the -- the first bolded heading, here it's talking about cyber attacks, the risk of cyber attacks?
A. Yes. Yes.
Q. And in the second sentence, it says (as read):
> Our systems and those of our third party service providers are vulnerable to, among other things, traditional computer hackers, malicious code, denial of service attacks, sophisticated nation state and nation state supported actors.

All of those are risks that were disclosed to investors?
A. Yes.
Q. And then in the fourth paragraph in the second sentence, it says (as read):
> Despite our security measures, unauthorized access to or security breaches of our software or systems could result in the loss, compromise or corruption of data,

investment -- investing public and expect them to -- to figure out whether there's a material weakness or not?

A. Yes. And that, I think, is important to highlight, which is there are a lot of -- there's a lot that takes to run a company. Some of it isn't necessarily get -- should get to our level because it becomes data that isn't material to how we would look at a company. So I think that line has to be determined by your own internal legal team and your CIO and CICO -- to make that determination.

Q. And you haven't seen any evidence of such a determination was made in any of the documents you've seen today?

A. None.

MR. TURNER: No further questions.

MR. BRUCKMANN: Nothing further from the SEC. I think we are done for today.

THE REPORTER: Could I just ask if anyone needs a transcript or a rough?

MR. TURNER: Yes, I'd like a rough, please.

MR. BRUCKMANN: We'll take the rough, yeah.

MR. BRUTLAG: I want to make sure, the

Latham & Watkins attorney, Christine Lee, joined as well, so you might want to include her on the attendees.

THE REPORTER: Thank you.

THE VIDEOGRAPHER: This concludes today's deposition of Brent Thill. Master media of today's deposition will remain in the custody of Gradillas Court Reporters. The time is 1:56 p.m. We are now off the record.

(Whereupon, the deposition concluded at 1:56 p .m.)

CERTIFICATE OF WITNESS

I, BRENT THILL, do hereby declare under penalty of perjury that I have read the entire foregoing transcript of my deposition testimony, or the same has been read to me, and certify that it is a true, correct and complete transcript of my testimony given on August 28, 2024, save and except for changes and/or corrections, if any, as indicated by me on the attached Errata Sheet, with the understanding that I offer these changes and/or corrections as if still under oath.

_____ I have made corrections to my deposition.

_____ I have NOT made any changes to my deposition.

Signed: _____
BRENT THILL

Dated this _____ day of _____ of 20____.

CERTIFICATE OF REPORTER

I, Kathleen A. Maltbie, Certified Shorthand Reporter licensed in the State of California, License No. 10068, the State of Nevada, CCR 995, and the State of Texas, CSR 12212, hereby certify that deponent was by me first duly sworn, and the foregoing testimony was reported by me and was thereafter transcribed with computer-aided transcription; that the foregoing is a full, complete, and true record of proceedings.

I further certify that I am not of counsel or attorney for either or any of the parties in the foregoing proceeding and caption named or in any way interested in the outcome of the cause in said caption.

The dismantling, unsealing, or unbinding of the original transcript will render the reporter's certificates null and void.

In witness whereof, I have hereunto set my hand this day:

_____ Reading and Signing was requested.
_____ Reading and Signing was waived.
___x___ Reading and Signing was not requested.

_____
KATHLEEN A. MALTBIE
RPR-RMR-CRR-CCRR-CLR-CRC-RDR
California CSR 10068, Nevada CCR 995
Texas CSR 12212